**In the Specification:**

Please amend the paragraph beginning on page 2, line 26 as follows:

If in a federated computing environment the authentication systems of all servers use one authentication policy (a concept including all user authentication forms, such as fingerprint authentication, voice print authentication and other authentication forms, rules in individual authentication forms (the number of characters, available term, data size, etc.), and combinations of them), a user may utilize the federated computing environment in such a manner that the user registers one group of authentication information items and perform user authentication by using his/her "unique" authentication information without being conscious of in which server he or she is using the authentication system. Thus, an authentication policy is defined as at least one rule for authenticating users of the federated computing environment.

Please amend the paragraph beginning on page 7, line 22 as follows:

The user authentication processing section 320 performs authentication processing according to an access request made by a user using the client 100 and received through communication control section 310. Preferably, the access request is implemented as an HTTP (HyperText Transfer Protocol) request generated in a Web browser in the client 100, sent out to the network 200 and received by the server 300, but is not limited. The user authentication processing section 320 includes an authentication request processing section 321, an authentication information management section 322, ~~an LDAP~~ a Lightweight Directory Access Protocol (LDAP) client 323, an authentication policy table 324, an exceptional ID table 325 and authentication information LDAP

326.

Please amend the paragraph beginning on page 9, line 1 as follows:

The authentication information management section 322 performs management of authentication information in the federated computing environment 1000. Preferably, the authentication information management section 322 has the function of performing processing for registering in the authentication policy table 324 of the authentication policies of the authentication systems of the servers included in the federated computing environment 1000, processing for updating the policies and processing for reference to the policies. The authentication information management section 322 also has the function of registering in the authentication information LDAP authentication information received from the user through the LDAP client 323. The authentication information management section 322 further has the function of determining, when ~~an user ID~~ a user indentification (ID) for a new user is registered, whether or not the same user ID has already been registered in the authentication system of any of the other servers using the same authentication policy, and registering the user ID in the exceptional ID table 325 if it determines that the same ID has been registered.

Please amend the paragraph beginning on page 11, line 15 as follows:

The exceptional ID table 325 is a table in which a user ID used by one user is registered as an exceptional ID if the same user ID is used by another user among the authentication systems of [[the]] at least two servers included in the federated computing environment 1000.

Please amend the paragraph beginning on page 12, line 6 as follows:

Figure 3 is a flowchart showing the flow of operations for establishing trusting relationships among the plurality of servers. In this embodiment, in a case where relationships of mutual trust are established among the plurality of servers 300-1 to 300-N, the server 300-1 first establishes, by the flow of operations shown in Figure [[4]] 3, trusting relationships with the server 300-2 to 300-N with which it has established no trusting relationships. Subsequently, the server 300-2 also establishes, by the flow of operations shown in Figure 4, trusting relationships with the server 300-3 to 300-N with which it has established no trusting relationships. This process is repeated to processing in the server 300-(N-1) to establish relationships of mutual trust among all the plurality of servers 300-1 to 300-N, thus forming the federated computing environment 1000.

Please amend the paragraph beginning on page 13, line 10 as follows:

If it is determined in S3040 that the authentication policy of the server 300-1 and the authentication policy of the server 300-2 are identical, an advance to S3050 corresponding to the arrow for "Yes" is made to examine whether or not [[one] a common user ID exists both in the authentication information LDAP 326 in the server 300-1 and in the authentication information LDAP 326 in the server 300-2. If it is determined in S3050 that no common user ID exists both in the authentication information LDAP 326 in the server 300-1 and in the authentication information LDAP 326 in the server 300-2, a move to S3090 corresponding to the arrow for "No" is made for determination as to whether or not a trusting relationship is still to be established with one of the other servers.

Please amend the paragraph beginning on page 13, line 22 as follows:

If it is determined in S3050 that [[one]] a common user ID exists both in the authentication information LDAP in the server 300-1 and in the authentication information LDAP in the server 300-2, an advance to step S3060 corresponding to the arrow for "Yes" is made to display an exceptional ID registration check frame shown in Figure 6 on the terminal operated by the system administrator attempting to establish a trusting relationship between the servers. In this embodiment, if a user ID "ABC001" is registered in both the server 300-1 and the server 300-2, the system administrator is asked to check whether or not the user ID are used by one user. In the exceptional ID registration check frame, registered names ("Tanaka Taro" provided as a registration name in combination with the user ID "ABC001" in the server 300-1, and "Hirota Keisuke" provided as a registration name in combination with the user ID "ABC001" in the server 300-2) are displayed as a hint for check to be presented to the system administrator, while being related to the server names and the user ID.

Please amend the paragraph beginning on page 14, line 23 as follows:

In S3090, determination is made as to whether or not a trusting relationship is still to be established with one of the other servers in the server 300-1. If it is determined in S3090 that a trusting relationship is still to be established with one of the other servers, a return to ~~S3030~~ S3020 in the flow is made and the steps ~~S3030~~ S3020 to S3080 are executed with respect to the server with which no trusting relationship has been established. The server 300-1 thus establishes trusting relationships with all of the other servers 300-2 to 300-N. If it is determined in S3090 that a trusting relationship is not still to be established with ~~none~~ any of the other servers, an advance in the flow corresponding to the arrow for ~~"Yes"~~ "No" and the flow ends.

Please amend the paragraph beginning on page 18, line 9 as follows:

The server 300-1 receives an access request from the user (S5010) for accessing the federated computing environment. In a case where the server 300-1 determines that the user sending the access request is unauthenticated by examining whether or not the security token is included in the access request, the server 300-1 transmits data on an authentication mode selection frame shown in Figure 7 to the client operated by the user to ask the user to select an authentication mode (S5020). If the user selects a multiple authentication mode by pressing a "Yes" button in the authentication mode selection frame shown in Figure 7 by way of example, the process advances to S5040. If the user selects a normal authentication mode by pressing a "No" button in the authentication mode selection frame shown in Figure 7 by way of example, the process moves to S5030 and user authentication is performed as normal authentication without using the authentication policy table. Since the normal authentication is well known, no detailed description will be made of the normal authentication.

Please amend the paragraph beginning on page 19, line 16 as follows:

The process advances to ~~S5050~~ S5060 and the server 300-1 obtains, by referring to its authentication policy table, addresses for one or more servers using the authentication policy matching the authentication information input by the user (S5060). For example, in a case where the server 300-1 uses the authentication policy table shown in Figure 9 and the authentication information includes a user ID "XYZ001" and a password "WXYZ", the authentication information matches the authentication policy using a user ID formed of "three alphabetic characters + three numeric characters" and a password formed of "four alphabetic characters", and the server 300-1 therefore

obtains three addresses "server300-1.com", "server300-2.com" and "server300-3.com".

Please amend the paragraph beginning on page 20, line 2 as follows:

This embodiment of the present invention has been described with respect to a mode in which a credential and cookie are used to permit a user to access the federated computing environment. However, it is apparent to those skilled in the art that URL encoding, or an ~~SAML~~ Security Assertion Markup Language (SAML) token or any other well-known authentication technique can be used as an alternative to the credential and cookie.